



**RECEIVED**  
**CENTRAL FAX CENTER**

NOV 19 2008

ATTORNEYS AT LAW  
402 W. BROADWAY, SUITE 2100  
SAN DIEGO, CA 92101.3542  
TELEPHONE: 619.234.6655  
FACSIMILE: 619.234.3510  
WWW.FOLEY.COM

**FACSIMILE TRANSMISSION****Total # of Pages 6 (including this page)**

TO:	PHONE #:	FAX #:
Examiner Jason Gee United States Patent & Trademark Office	571-272-6431	571-273-8300

From : Sanjeev K. Dhand  
Email Address : sdhand@foley.com  
Sender's Direct Dial : 858.847.6860  
Date : November 19, 2008  
Client/Matter No : 061715-0391  
User ID No :

**MESSAGE:**

Re: Application Number 10/679,486

Examiner: Jason Gee

Art Unit: 2434

Included in this facsimile are:

- Interview Agenda (1 page)
- Proposed Claim Amendments (4 pages)

If there are any problems with this transmission or if you have not  
received all of the pages, please call 619.234.6655.

Operator:	Time Sent:	Return Original To: Juliene P. Britt
-----------	------------	-----------------------------------------

CONFIDENTIALITY NOTICE: THE INFORMATION CONTAINED IN THIS FACSIMILE MESSAGE IS INTENDED ONLY FOR THE PERSONAL AND CONFIDENTIAL USE OF THE DESIGNATED RECIPIENTS NAMED ABOVE. THIS MESSAGE MAY BE AN ATTORNEY-CLIENT COMMUNICATION, AND AS SUCH IS PRIVILEGED AND CONFIDENTIAL. IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT OR ANY AGENT RESPONSIBLE FOR DELIVERING IT TO THE INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED THAT YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, AND THAT ANY REVIEW, DISSEMINATION, DISTRIBUTION OR COPYING OF THIS MESSAGE IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS COMMUNICATION IN ERROR, PLEASE NOTIFY US IMMEDIATELY BY TELEPHONE AND RETURN THE ORIGINAL MESSAGE TO US BY MAIL. THANK YOU.

Cover Page 1 of 1

NOV. 19. 2008 6:02PM

FOLEY 8587926773

RECEIVED  
CENTRAL FAX CENTER

NO. 8565 P. 2

NOV 19 2008

PTOL-413A (10-08)  
Approved for use through 11/30/2008. OMB 0651-0031  
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE**Applicant Initiated Interview Request Form**

Application No.: 10/679,486 First Named Applicant: Pienimaki  
 Examiner: Jason Gee Art Unit: 2434 Status of Application: pending

**Tentative Participants:**

(1) Sanjeev K. Dhand (2) \_\_\_\_\_  
 (3) \_\_\_\_\_ (4) \_\_\_\_\_

Proposed Date of Interview: November 24, 2008 Proposed Time: 1 PM (EST) AM/PM

**Type of Interview Requested:**

(1) ☒ Telephonic (2) ☐ Personal (3) ☐ Video Conference

Exhibit To Be Shown or Demonstrated: ☐ YES ☒ NO

If yes, provide brief description: \_\_\_\_\_

**Issues To Be Discussed**

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) <u>35 USC 102(e)</u>	<u>1,2, 5-12</u>	<u>Wu</u>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(2) _____	_____	_____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(3) _____	_____	_____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(4) _____	_____	_____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ Continuation Sheet Attached

**Brief Description of Argument to be Presented:**

Singular entity (access control point) performs AAA procedure and traffic encryption enforcement

An interview was conducted on the above-identified application on \_\_\_\_\_.

**NOTE:** This form should be completed by applicant and submitted to the examiner in advance of the interview (see MPEP § 713.01).

This application will not be delayed from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible.

\_\_\_\_\_  
 Applicant/Applicant's Representative Signature

Sanjeev K. Dhand

\_\_\_\_\_  
 Typed/Printed Name of Applicant or Representative  
51,182

\_\_\_\_\_  
 Registration Number, if applicable

\_\_\_\_\_  
 Examiner/SPE Signature

This collection of information is required by 37 CFR 1.133. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 1.

NOV 19 2008

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicant: PIENIMAKI et al.  
Title: FORCED ENCRYPTION FOR  
WIRELESS LOCAL AREA  
NETWORKS  
Appl. No.: 10/679,486  
Filing Date: 10/7/2003  
Examiner: Jason Gee  
Art Unit: 2434  
Confirmation Number: 4042

**PROPOSED AMENDMENTS FOR EXAMINER INTERVIEW**

Mail Stop Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

This communication is responsive to the Final Office Action dated October 10, 2008, concerning the above-referenced patent application.

The following are proposed amendments to be discussed in the November 24, 2008 telephonic Examiner Interview.

**Amendments to the Claims** are reflected in the listing of claims which begins on page 2 of this document.

**RECEIVED  
CENTRAL FAX CENTER**

**NOV 19 2008**

**Proposed Amendments to the Claims:**

1. (Currently Amended) A method, comprising:
  - providing access to accessing a public wireless local area network for a user terminal;
  - initiating an authentication, authorization and accounting procedure for the user terminal;
  - providing an internet access gateway functionality; and
  - enforcing an application to switch any traffic provided over internet access to the user terminal in the public wireless local area network to an encrypting security service port, wherein the initiating and enforcing are performed by an access control point.
2. (Original) The method according to claim 1, wherein the encrypting security service is the secure sockets layer or the transport layer security.
3. (Canceled).
4. (Canceled).
5. (Previously Presented) The method according to claim 1, further comprising:
  - retrieving information from RADIUS messages whether a user terminal does not use a 802.11i encryption; and
  - performing the enforcing to the application if it is accessed by such a user terminal.
6. (Previously Presented) The method according to claim 1, wherein the application can be one of a group comprising the hypertext transfer protocol for browsing the Internet, the Internet message access protocol 4, the post office protocol 3, and the simple mail transfer protocol.
7. (Currently Amended) An apparatus, comprising:
  - means for controlling access to a public wireless local area network

means for initiating an authentication, authorization and accounting procedure for a user terminal

means for providing an internet access gateway functionality; and

said means for initiating being configured to enforce enforcing an application accessed by the user terminal via the internet to switch any traffic to an encrypting security service port.

8. (Previously Presented) The apparatus according to claim 7, wherein the encrypting security service is the secure sockets layer or the transport layer security.

9. (Previously Presented) The apparatus according to claim 7, further comprising:

means for retrieving information from RADIUS messages whether the user terminal does not use a 802.11i encryption; and

means for enforcing the application if it is accessed by such a user terminal.

10. (Currently Amended) An apparatus, comprising:

a wireless local area network controller configured to control access to a public wireless local area network;

an authentication, authorization and accounting controller configured to initiate an authentication, authorization and accounting procedure for a user terminal; and

an access gateway controller configured to provide an internet access gateway functionality; [[and]]

wherein the authentication, authorization and accounting controller is further a processor configured to enforce an application accessed to by the user terminal via the internet to switch any traffic to an encrypting security service port.

11. (Previously Presented) The apparatus according to claim 10, wherein the encrypting security service is the secure sockets layer or the transport layer security.

12. (Previously Presented) The apparatus according to claim 10, further comprising:

a transceiver configured to retrieve information from RADIUS messages whether the user terminal does not use a 802.11i encryption; [[and]]

wherein the processor is further configured to enforce the application if it is accessed by such a user terminal.